(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 740 037 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.10.1996 Bulletin 1996/44

(51) Int. Cl.[6]: **E05B 49/00**

(21) Application number: **95302889.1**

(22) Date of filing: **28.04.1995**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant: **Hewlett-Packard Company**
Palo Alto, California 94304 (US)

(72) Inventor: **Proudler, Graeme John**
Stoke Gifford, Bristol BS12 6XQ (GB)

(74) Representative: **Newell, William Joseph et al**
Wynne-Jones, Lainé & James
22 Rodney Road
Cheltenham Gloucestershire GL50 1JJ (GB)

(54) Security device

(57) A security device 16 for deterring theft of the equipment 10 into which it is incorporated is embedded in an ASIC 11 which controls many of the functions of the equipment 10. The security device periodically implements a challenge/response routine with a remote security centre 20. If the appropriate response is not received, the security device 16 disables the ASIC 11, so that the equipment 10 does not operate properly. On detecting theft of the equipment 10 the user contacts the security centre to hold the response when next challenged.

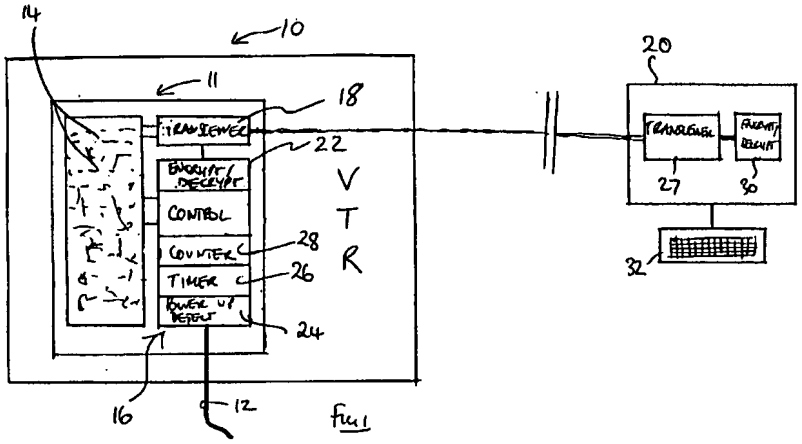

Fig 1

EP 0 740 037 A1

Description

FIELD OF THE INVENTION

This invention relates to a security device for deterring theft of the apparatus or equipment to which it is fitted or into which it is incorporated.

BACKGROUND TO THE INVENTION

Various proposals exist to render stolen equipment inoperable and thus prevent use by the thief. Some automobile audio systems include a feature whereby on interruption of the power supply, for example due to temporary or permanent removal from the automobile, the audio system will not function properly until a code is keyed in. There also exist schemes in which an automobile is fitted with an immobiliser which is activated on receipt of an instruction from a remote security centre. Elsewhere it has been proposed to provide electronic goods such as televisions, video tape recorders, etc with a disabling unit which can be activated by a remote control station.

However, these latter systems all require the remote control station to issue a signal instructing immobilisation or disablement, and so are not effective if the stolen equipment is taken outside the range of the remote station, or if communication with the remote unit is deliberately or otherwise broken. Furthermore, the security of these systems may be circumvented by the reasonably knowledgeable crook by by-passing the disabling unit or immobiliser.

SUMMARY OF THE INVENTION

We have designed a system in which the equipment to which the security device is fitted periodically initiates a validation routine which, to be completed successfully, requires a specific instruction signal from a security station.

Accordingly, in one aspect, this invention provides a security device for use with apparatus and for allowing continued operation of said apparatus dependent on a specific instruction signal from a security station, said device including signal receiving means for receiving a specific instruction signal from said security station and interrupt means responsive to said signal receiving means in a validation routine for inhibiting, preventing, or interfering with operation of said apparatus if said specific instruction signal is not received.

Thus in this device, if the owner has notified the security station that the apparatus has been stolen, the security station will ensure that the appropriate instruction is not transmitted in the next validation routine and so the apparatus will not function properly thereafter. Also, if for any reason the apparatus is not in communication with the remote centre during a validation routine, it will not function properly.

In a simple system there may be only one-way communication from the remote centre to the security device, to provide just the required specific instruction signal, with the initiation of the validation routine being effected indirectly, perhaps by the device alerting the owner to contact the remote station by telephone. However it is preferred for this to be done automatically, with the security device including signal transmitting means for transmitting a challenge signal to request said security station to transmit said specific instruction signal.

The device preferably implements a challenge/response routine, whereby the specific instruction signal issued by said security station is a specific response to said challenge signal, and the security device includes means for authenticating said specific response signal.

The challenge and response signals are preferably encrypted on transmission and decrypted on receipt. The security device preferably includes secure memory means, such as a Write Once Read Many (WORM) memory accessible only internally by the security device for storing one or more keys for use in the encryption/decryption process. The encryption/decryption process may be any one of several suitable types, for example public key or symmetric key systems.

Preferably, communication between said security device and said security station is via a communications network, and said challenge signal includes data identifying the network address of said security device, whereby the security centre may determine the logical location of a security device, and send the response signal to that location.

The security device is preferably incorporated in an integrated circuit which in use exerts at least a major part of the control function of the equipment. As integrated circuit technology develops further, so more and more functionality is integrated into larger and larger chips, and preferred embodiments take advantage of this by incorporating the security device into an application specific integrated circuit (ASIC) together with circuits representing most of the functionality of the equipment. This provides an important level of security as it is extremely difficult, if not virtually impossible, for someone to circumvent the security device, at least at economically realistic levels.

A further point is that it is highly desirable that a security system does not interfere with routine maintenance and repair of equipment, for example by restricting supply of replacement chips to legitimate owners or service personnel. Thus, if the security device is securely embedded into the ASIC, ready availability of replacement ASICs should not significantly degrade security of the system, because by their design the replacement ASICs will also require periodic permission from the security station, to function properly.

There are various ways of ensuring that the security device checks routinely for an instruction signal from the security station. Thus, if the apparatus is connected to power permanently or for long periods, the device pref-

erably includes a timer and initiates a validation routine each time the timer times out. Alternatively, or in addition, where the apparatus is operated for shorter periods, the device may include a non volatile counter means which increments each time the apparatus is operated or powered up, the device initiating a validation routine every time the counter means reaches a predetermined number or multiple thereof.

Communication between the security device and the security station may be set up in a variety of ways. For apparatus such as a video tape recorder which is semi-permanently located, communications may be via the plain old telephone system (POTS). For other applications, e.g. with mobile equipment or vehicles, communication may be via a cellular telephone network, radio, infra-red data links and so on, or combinations of these, and suitable communication systems will be apparent to those skilled in the art.

Whilst the invention has been described above, it extends to any inventive combination of the features set out above or in the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may be performed in various ways and, by way of example only, an embodiment thereof will now be described in detail, reference being made to the accompanying drawings, in which:-

Figure 1 is a schematic diagram of equipment fitted with an embodiment of security device in accordance with this invention, and

Figure 2 is a flow chart showing the operation of the security device of Figure 1.

DESCRIPTION OF THE PREFERRED EMBODIMENT

In this example, the security device 16 is incorporated in a video tape recorder (VTR) 10, semi-permanently connected to a power supply by lead 12. The VTR 10 follows conventional design except that most of the functionality of the apparatus is integrated into an application specific integrated circuit (ASIC) 11. Thus the ASIC has a collection of functional circuit elements 14 which control most of the mechanical and electrical functions such as tape and cassette transport, tuning, programming, timing, etc operations, to the extent that the VTR 10 has minimal resale value without a fully functional ASIC 11. The ASIC 11 also includes a security device 16 which is capable of disrupting operation of at least some of the functional circuit elements 14, if certain security conditions are not met, to be described in further detail below. The disruption may take the form of inhibiting some or all of the responses to controls and disabling some or all outputs of the functional circuit elements. This may be done, for example, by forcing internal signals to a quiescent state, removal of scanning waveforms, forcing incoming control signals to their quiescent state, forcing outputs to their quiescent sate, removing clock or power from certain internal circuits, or stopping a microprocessor from executing normal operations by the use of a conditional test input or interrupt input. These actions may be forced at various functional circuit elements 14 within the ASIC 11 by control signals. ASIC conductors are usually difficult to isolate and it is usually difficult to make an electrical connection to those conductors. However, in this embodiment they may be buried within the volume of the ASIC 11, so that they cannot be accessed without irreparably damaging other elements of the ASIC 11, further to enhance security.

There may be multiple conductors, each providing the permission signal to different functional circuit elements 14, each driven by a separate buried buffer from within the security device, so that multiple connections must be made to override the 'stop' signal. Each functional circuit element may contain a communication element for communication with the security device 16, such that each communication element may requires a waveform, rather than a simple logic level, to allow operation. Each communication element may require a different waveform so that active inputs, rather than logic levels, are required to override the 'stop' signal. Thus the level of complexity, and thus immunity to interference may be selected according to the level of perceived threat.

Although for ease of illustration the functional circuit elements 14 are shown discrete from the security device 16, in practice the circuit elements may be interspersed, to minimize the possibility of successfully circumventing the operation of the security device 16, as discussed above.

The security device 16 has a transceiver 18, capable of transmitting and receiving signals to and from a remote security centre 20, by any suitable communication medium, here the POTS system. Although shown on the ASIC 11, the transceiver 18 may be separate. The security device 16 also includes circuitry 22 for implementing a challenge/response scheme based on cryptographic techniques, and storing the associated encryption data. Such encryption systems are well known, see for example page 357 - "Peer Entity Authentication" in "Security for Computer Networks" Davies and Price, John Wiley and Sons, 2nd Edition, 1989, and ISO 9798 "Peer Entity Authentication Mechanism Using An n-bit Secret Key". There are many possible challenge/response mechanisms. They are of varying degrees of complexity, but the general basis is for the security device 16 to obtain a random number, encrypt it using a first key, K1, and send it to the remote security centre 20. This is the challenge. The remote security centre 20 decrypts the challenge with the key K1, encrypts it with a second key, K2, and sends it back to the security device. This is the response. The security device decrypts the response with key K2 and checks that the decrypted number is the same as the original random number. This proves to the security device that

the message came from an entity with knowledge of the keys K1 and K2, presumed to be the remote security centre 20. The remote security centre 20 provides the response only if the security device 16 is authorized to continue operation. Thus encryption systems such as public key, symmetric key etc. may be used.

The security device 16 also includes power-up detect circuitry 24 which detects power up of the ASIC 11, a timer 26 and a non-volatile counter 28. The ASIC 11 contains a write once read many memory (WORM), which is preferably a fusible link device, although it could be an EPROM in a non-transparent package.

The remote security centre 20 serves many units in an area and includes a transceiver 27 for transmitting and receiving signals to and from the units containing the ASIC 11 via the POTS system. It also includes circuitry 30 for implementing cryptographic techniques and for storing the associated encryption data, and an operator interface 32 which allows the operator to prevent transmission of response signals to a selected unit, if that unit has been identified as stolen.

In operation of the system, when leaving the factory, the ASIC 11 is programmed with a key pair preferably in the WORM and the associated key pair is registered with a central agency which runs the remote security centre 20. Referring to Figure 2, when the VTR 10 is turned on, the non-volatile counter 28 is incremented and the device determines whether the counter has reached the predetermined number or a multiple thereof (Steps 40, 42).

If the counter 28 has reached the number or a multiple, the device initiates a validation routine by calling up the remote security centre 20, issuing a challenge and requesting a response using the encryption and decryption steps referred to above. Unless the remote security centre 20 has been advised that the VTR 10 has been stolen, the centre will respond with a response which is then checked by the security device 16 to ensure that it is as expected and, if so, the device allows the VTR 10 to continue to operate. The timer 26 and counter 28 are then reset at step 44, and the device goes into a timed routine 46.

If the VTR 10 has been disconnected from the communication medium, or the remote security centre 20 has been alerted not to send the response, non-arrival of the response triggers the safety device 16 at step 48 to stop normal operation of the VTR 10 using one of the disruption techniques described above, and to wait for possible manual initiation of the validation routine.

If on detection of power up, the counter 28 does not reach the preset number, then it goes into the timed routine 46. Here the timer 26 runs until it times out, whereupon the security device 16 initiates the validation routine by calling up the remote centre 20.

As soon as a legitimate owner becomes aware of the theft of equipment incorporating the security device 16, he calls up the agency running the remote security centre 20 which, after appropriate checks, instructs the remote security centre not to send any response signal to the stolen equipment. The equipment, even if connected to the appropriate communication medium, will become non-functional and of minimal resale value when the security device is triggered by non-arrival of the response signal.

As a development of this system, the challenge issued by the security device 16 may include data representing the identity or location of the user, such as the source network address of the security device (for example the user's telephone number, if communications are via the POTS). The remote security centre 20 would then send the response back to that same network address, possibly after a deliberate break in communication. This would allow the remote security centre 20 to monitor the logical location of the security device 16, and possibly provide a tracking facility.

Claims

1. A security device for use with apparatus and for allowing continued operation of said apparatus dependent on a specific instruction signal from a security station, said device including signal receiving means for receiving a specific instruction signal from said security station and interrupt means responsive to said signal receiving means in a validation routine for inhibiting, preventing, or interfering with operation of said apparatus if said specific instruction signal is not received.

2. A security device according to Claim 1, wherein said security device includes signal transmitting means for transmitting a challenge signal, to request said security station to transmit said specific instruction signal.

3. A security device according to Claim 2, wherein in use said security device and said security station communicate via a communications network, and said challenge signal includes data identifying the network address of said security device.

4. A security device according to any preceding Claim, wherein said specific instruction signal from said security station comprises a specific response signal to said challenge signal, and said security device includes means for authenticating said specific response signal.

5. A security device according to Claim 4, including means for encrypting said challenge signal.

6. A security device according to Claim 4 or Claim 5, wherein said specific response is in encrypted form, and said device includes means for decrypting said specific response.

7. A security device according to Claim 5 or Claim 6, including a secure memory for storing one or more keys for said encryption process.

8. A security device according to any preceding Claim, wherein said interrupt means is incorporated in an integrated circuit which also contains circuitry which exerts a control function in the apparatus.

9. A security device according to Claim 8, wherein said integrated circuit contains at least a major part of the control function of the apparatus.

10. A security device according to any preceding Claim, wherein said security device includes timer means which, on timing out, initiates said validation routine.

11. A security device according to any preceding Claim, wherein said security device includes power-up detection means for detecting power-up of said apparatus, and non-volatile counter means for being incremented at each power-up and for initiating said validation routine when the count on said counter means reaches a predetermined number or multiple thereof.

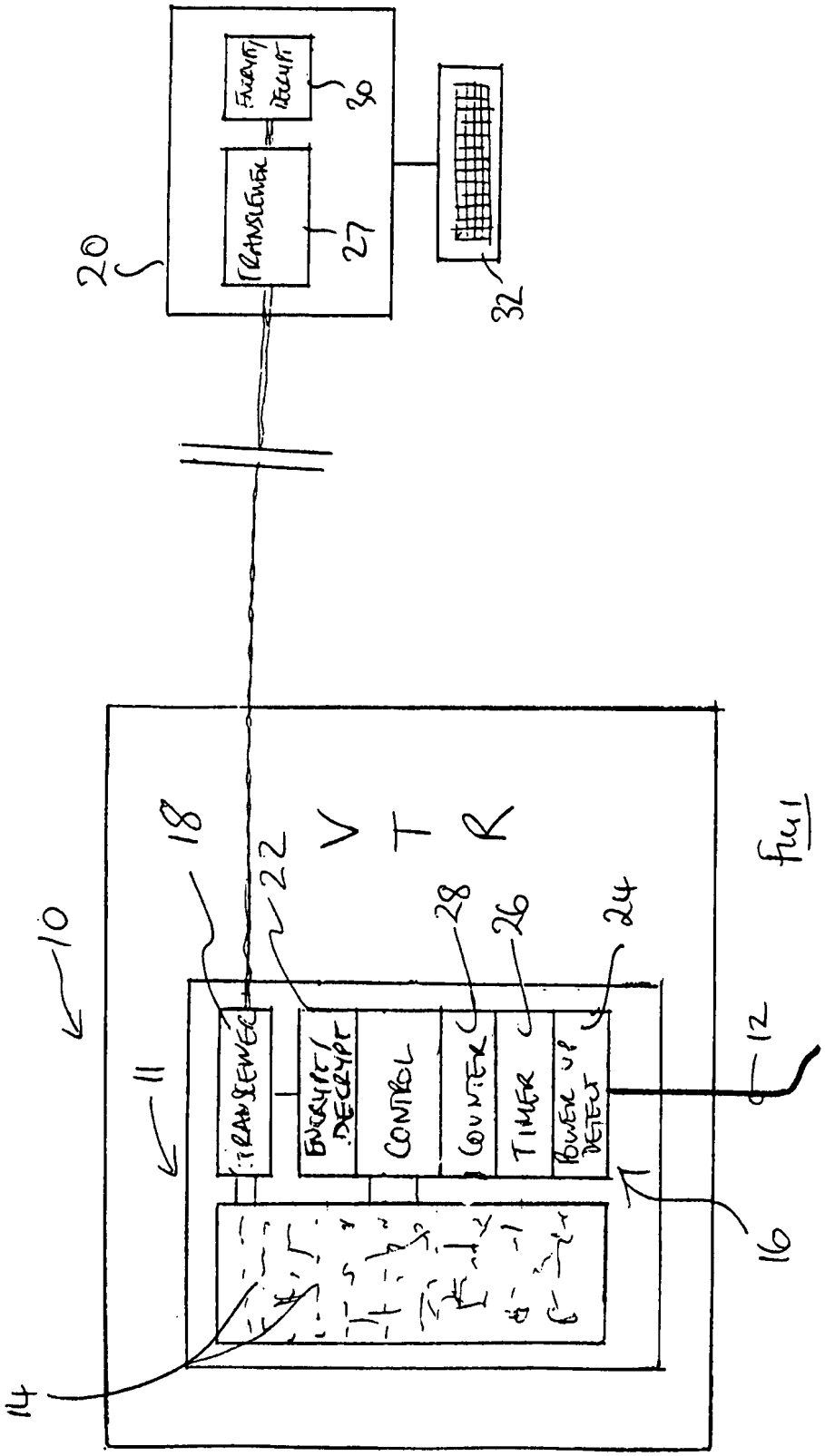
20
TRANSCEIVER
27
ENERGY DETECT
30
32
10
11
18
22
28
26
24
TRANSCEIVER
ENCRYPT/DECRYPT
CONTROL
COUNTER
TIMER
POWER UP DETECT
12
14
16
V
T
R

Fig 1

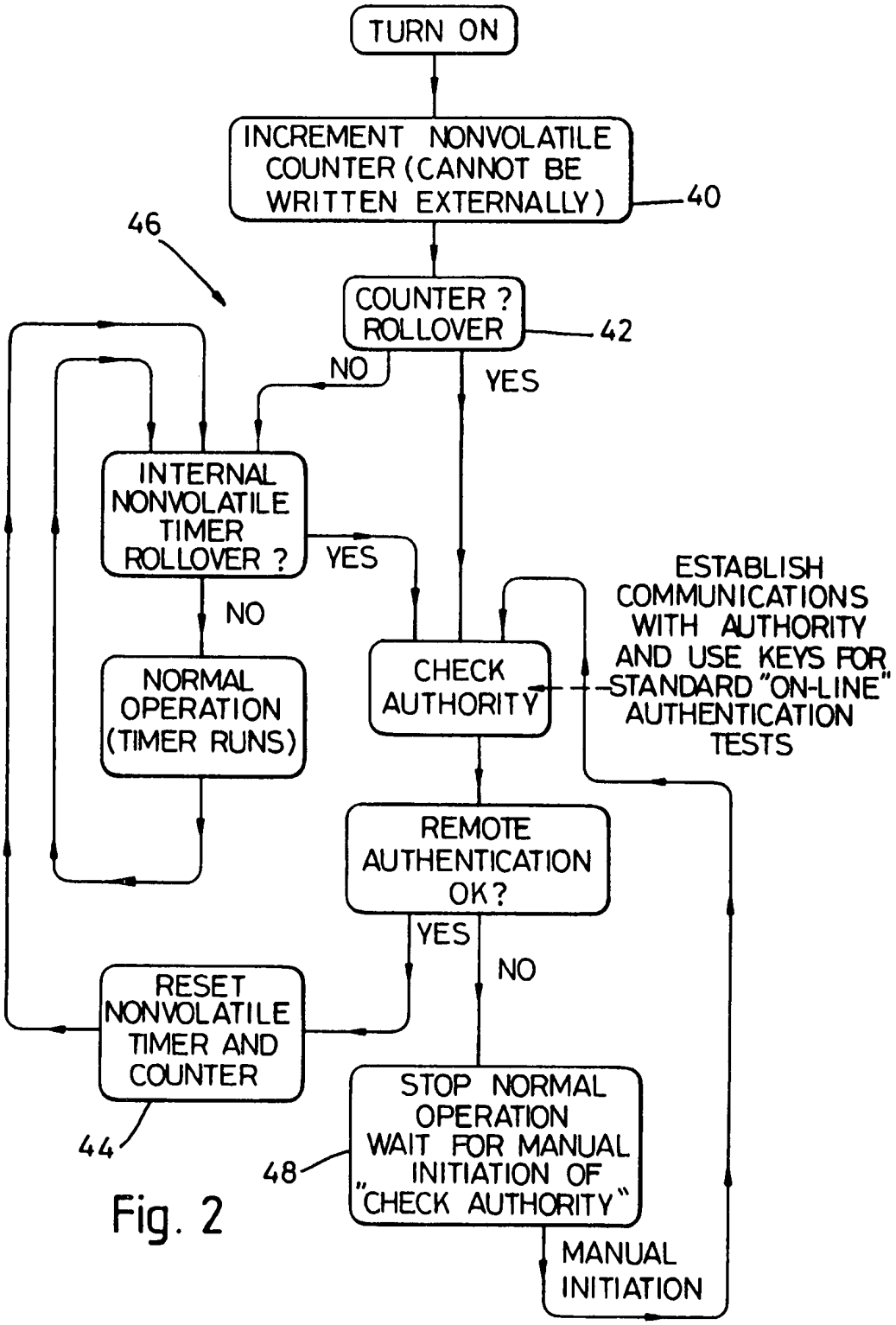
TURN ON
INCREMENT NONVOLATILE COUNTER (CANNOT BE WRITTEN EXTERNALLY)
40
46
COUNTER ? ROLLOVER
42
NO
YES
INTERNAL NONVOLATILE TIMER ROLLOVER ?
YES
NO
NORMAL OPERATION (TIMER RUNS)
CHECK AUTHORITY
ESTABLISH COMMUNICATIONS WITH AUTHORITY AND USE KEYS FOR STANDARD "ON-LINE" AUTHENTICATION TESTS
REMOTE AUTHENTICATION OK?
YES
NO
RESET NONVOLATILE TIMER AND COUNTER
44
STOP NORMAL OPERATION WAIT FOR MANUAL INITIATION OF "CHECK AUTHORITY"
48
MANUAL INITIATION

Fig. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 30 2889

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	EP-A-0 387 581 (BLAUPUNKT-WERKE GMBH.) * abstract; figures 1,2 * * column 2, line 40 - column 3, line 3 * * column 3, line 25 - line 39 *	1,2,4-6	E05B49/00
Y	GB-A-2 262 640 (INTELLIGENT LOCKING SYSTEMS LTD.) * abstract; figures 1,2 * * page 6, line 16 - line 30 * * page 12, line 6 - line 15 *	1,2,4-6	
A	US-A-4 794 268 (NAKANO ET AL.) * abstract; figures 1,4 * * column 3, line 57 - column 4, line 21 *	1	
A	DE-A-39 27 024 (NISSAN MOTOR CO. LTD) * the whole document *		
A	EP-A-0 135 783 (NEC CORP.) * the whole document *		
			TECHNICAL FIELDS SEARCHED (Int.Cl.6) E05B G08B B60R

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	26 September 1995	Danielidis, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)